**Техническое задание**

**Тестирование SS7 (ОКС №7) ООО «Скай Мобайл»**

1. **Введение**

Цель данного тестирования состоит в проверке эффективности и надежности Signalling Firewall SS7, предназначенного для защиты сети от угроз безопасности, связанных с протоколом SS7. Тестирование на проникновение Signalling Firewall SS7 включает в себя проведение активных атак с целью проверки устойчивости и эффективности защитных механизмов, а также выявления потенциальных уязвимостей.

1. **Объекты тестирования**

* Signalling Firewall SS7, установленный в сети SS7.
* Сетевые элементы, работающие по протоколу SS7, включая коммутаторы, маршрутизаторы и сигнализационные центры (STP).
* Интерфейсы передачи сигнализации, такие как E1/T1, SCTP/IP и M3UA/SUA, а также более актуальных версий интерфейсов.

1. **Требования к тестированию**
   1. **Идентификация уязвимостей**

* Анализ конфигурации Signalling Firewall SS7 на наличие уязвимостей и неправильных настроек.
* Проверка целостности и защиты конфигурационных файлов и баз данных Signaling Firewall SS7. Оценка наличия защиты от несанкционированного изменения конфигурации и БД Signaling Firewall SS7.
* Проверка возможности обхода или обнаружения слабых мест в защите Signalling Firewall SS7.
* Оценка эффективности механизмов аутентификации и авторизации в Signalling Firewall SS7.
  1. **Активные атаки**
* Тестирование всех векторов атак на SS7 (проверка сети, сбор абонентских данных (IMSI, MSC/VLR, HLR), отслеживание местоположений абонентов, перехват звонков и SMS-сообщений, отправка поддельных SMS и USSD-сообщений, DOS абонента или сегмента сотовой связи).
* Проведение атак на Signalling Firewall SS7 с целью обхода или обнаружения его защитных механизмов.
* Проверка возможности проникновения в сеть SS7 через уязвимые точки Signalling Firewall SS7.
* Оценка способности Signalling Firewall SS7 обнаруживать и предотвращать активные атаки на сеть SS7.
* Оценка времени обнаружения и реагирования Signalling Firewall SS7 на потенциальные угрозы и атаки.
* Обязательное тестирование и экпслуатация наиболее популярных атак на SS7, перечисленных в Приложении 1.
* Атака на отказ в обслуживании(DoS), направленную на сеть. Отправка большого объема трафика, манипуляция сигнальными сообщениями или другими действиями, которые могут вызвать отказ в работе сети. Как Signaling Firewall SS7 обнаруживает и справляется с такими атаками, сохраняя работоспособность сети.
* Атака на управление услугами. Изменение настроек (отключение и подключение услуг) и параметров услуг.

1. **Технический анализ**

* Анализ разрешенных и заблокированных служб и протоколов. Убедиться, что только необходимые протоколы и службы разрешены, ненужные заблокированы.
* Оценка механизмов оповещения пользователей.
* Журналирование и анализ. Проверка каким образом Signaling Firewall SS7 осуществляет журналирование событий и действий, связанных с угрозами и атаками.
* Проверка фильтров сигнальных сообщений. Проверка блокировки некорректно сформированных (malformed) пакетов.
* SS7 signaling spoofing. Проверка блокировки поддельных сигнальных сообщений.
* Проверка защиты от фальсификации номеров вызывающих абонентов.

1. **Квалификация**

* Тестирование на проникновение Signalling Firewall SS7 должно быть проведено квалифицированными специалистами в области безопасности сетей и протоколов передачи данных.
* Исполнители должны иметь обязательный опыт в проведении аналогичных аудитов (не менее 2 подобного рода проектов в Телекоммуникационной отрасли).
* Специалисты Исполнителя должны иметь знания в области SS7, SigTRAN and SIP Security, а также иметь подтверждающие квалификацию сертификаты.
* Специалисты Исполнителя должна обладать следующими статусами:

- OSCP, Certified Information System Auditor (CISA), Certified Information Systems Security Professional (CISSP).

* Исполнитель должен иметь не менее трех аналогичных завершенных проектов.
* В организационно-штатной структуре Исполнителя должно быть выделенное подразделение, отвечающее за работы в области информационной безопасности.
* Исполнитель должен предоставить описание проектной команды, которое должно включать следующую информацию по каждому члену команды: описание роли в проектной команде, перечень решаемых задач, перечень сертификатов, подтверждающих компетентность данного члена команды по данному направлению.

1. **Разработка рекомендаций** 
   1. **Рекомендаций по устранению выявленных замечаний разрабатываются с учётом следующих направлений:**

* изменение конфигураций существующих средств защиты.
* рекомендации по внедрению и настройке средств защиты информации (как общедоступных, так и коммерческих решений).

Результатом работ на данном этапе является План реализации организационных и технических мероприятий, выполнение которых позволит повысить текущий уровень безопасности.

1. **Документация**

* Формирование отчета о тестировании на проникновение Signalling Firewall SS7, включающего выявленные уязвимости, описание проведенных атак и рекомендации по улучшению безопасности.
* Предоставление дополнительной документации, включающей технические детали тестирования, использованные инструменты и методологию.
* Отчетная документация должна включать рекомендации по устранению выявленных уязвимостей. Рекомендации должны иметь полный мануал с описанием всех необходимых действий (установка патчей, настройка и т.д.).

**Результаты оказания услуг:**

На основании проведённого аудита предоставляется подробный отчет с перечнем выявленных    уязвимостей, несоответствий и рекомендаций, включающий в себя:

* + перечень выявленных угроз с оценкой и описанием рисков информационной безопасности;
  + рекомендации по минимизации выявленных рисков;
  + отчеты и рекомендации по всем системам и подсистемам, по которым была проведена работа;
  + Компании должна оказываться консалтинговая поддержка по вопросам информационной безопасности сроком на 1 год/

**Приложение 1. Популярные атаки на протокол SS7.**

1. **Раскрытие IMSI**. Данная атака осуществляется при помощи запроса адреса коммутатора, который обслуживает абонента в текущий момент времени. Запрос является частью процесса доставки SMS-сообщения; он позволяет оборудованию сети в которой был инициирован запрос получить данные о местоположении абонента для последующей доставки сообщения.
2. **Раскрытие местоположения абонента**. Данная атака осуществляется при помощи несанкционированного запроса о местоположении абонента. Полученные данные используются для онлайн-тарификации входящих вызовов абонента. Злоумышленник получает Cell Global Identity (CGI), который позволяет определить местоположение абонента с точностью в несколько сотен метров.
3. **Сбой в обслуживании**. В ходе данной атаки происходит регистрация абонента в новой зоне покрытия коммутатора. Аналогичная процедура происходит при регистрации абонента в сети оператора — партнера по роумингу. В результате атаки абонент перестает получать звонки или текстовые сообщения, хотя сам телефон при этом находится в зоне доступа.
4. **Перехват входящих SMS-сообщений**. Поддельная регистрация позволяет злоумышленнику перенаправлять все SMS-сообщения, предназначенные абоненту, на свой узел.
5. **Эксплуатация USSD-запросов**. Данная атака имитирует отправку сообщения с USSD-запросом от VLR к HLR. Наиболее опасный сценарий — отправка запроса на перевод денежных средств между счетами абонентов. В ходе анализа защищенности сети SS7 могут быть проверены следующие варианты атаки:

* раскрытие данных о балансе абонента;
* o перевод денежных средств между счетами абонентов.

1. **Перенаправление входящего вызова**. В ходе атаки происходит подмена роумингового номера, что позволяет злоумышленнику влиять на маршрутизацию голосовых вызовов в сети оператора. Этот метод может быть использован для перенаправления входящих вызовов абонента или осуществления звонков на дорогие направления за счёт оператора связи.
2. **Изменение категории оплаты**. В ходе атаки происходит подмена параметров VLR-CSI, отвечающих за онлайн-тарификацию, в профиле абонента. Если злоумышленник удаляет параметр VLR-CSI, платежная категория абонента меняется на постоплатную, а все последующие звонки обойдут систему онлайн-тарификации.
3. **Перенаправление исходящего вызова**. В ходе атаки происходит подмена адреса gsmSCF системы онлайн-тарификации в профиле абонента. Запрос об оплате всех исходящих вызовов направляется на адрес, введенный злоумышленником. Злоумышленник может перенаправить исходящий вызов на номер другого абонента.
4. **Обход существующих средств безопасности**. Попытки проведения выше указанных атак сообщениями или методиками, не попадающими под категории и рекомендации нормативной документации GSMA.